CYREBRO

Cybersecurity Regulatory Compliance Guide 2023

TABLE OF CONTENTS

Compliance Is Not a Choice

In recent years, organizations' attack surfaces have grown significantly due to remote work, rapid digitization, and a wealth of new collaboration tools, introducing new vulnerabilities and reducing visibility.

At the same time, bad actors are becoming more creative with attack methods, while ransomware gangs are growing and providing how-to kits that inexperienced threat actors can easily use. This has led to a critical junction. Cyber threats and data breaches are on the rise, with global attacks increasing by 38% in 2022 compared to 2021.

Governments and industries worldwide have responded by implementing stringent cybersecurity regulations and laws, which organizations must adhere to. However, for organizations that operate across borders, achieving compliance can feel as futile as attempting to find a needle in a needle stack. Nevertheless, compliance is not a choice, and the consequences of non-compliance can be devastating. Armed with the proper knowledge, tools, and strategies, organizations can meet compliance requirements.

This eBook can serve as a comprehensive guide to understanding the most common regulations from a global perspective. It covers why compliance is crucial, who needs to adhere to which standards, the challenges of compliance, how to build a robust cybersecurity compliance program, and how security solutions such as a Security Operations Center (SOC) come in handy.

What Is Cybersecurity Compliance?

Cybersecurity compliance is the practice of following regulations, standards, and guidelines set by government bodies and industry associations to safeguard digital information and infrastructure. These regulations are designed to protect sensitive data, ensure data privacy, and maintain the integrity and availability of information systems.

Cybersecurity compliance standards can encompass various aspects of data protection, security controls, incident response planning, and risk management. They provide a crucial framework for organizations to follow, promoting a robust cybersecurity posture.

CHAPTER 1:

Why Is Regulatory Compliance Important in Cybersecurity?

Compliance is a fundamental aspect of a comprehensive cybersecurity strategy and offers organizations numerous benefits:

LEGAL OBLIGATIONS: Organizations are legally bound to comply with regulations in their respective regions and industries. Failure to comply can result in severe penalties, including fines, lawsuits, and even imprisonment for individuals responsible for non-compliance.

RISK MITIGATION: By complying with the regulations, organizations implement security controls designed to protect their systems and data from attack, improving their overall security posture.

DATA PROTECTION: Compliance ensures that organizations implement adequate security measures to safeguard sensitive data from unauthorized access, breaches, and theft by establishing a framework for encryption, access controls, data retention policies, and data breach notification requirements.

TRUST AND REPUTATION: Compliance can give you a competitive edge in the marketplace as customers, clients, and partners are likelier to do business with organizations that protect sensitive information.

CHAPTER 2:

Who Should Comply With These Standards?

Cybersecurity regulations apply to a wide range of organizations, including businesses of all sizes, government agencies, healthcare providers, financial institutions, and more.

Generally, anyone who collects, processes, or stores sensitive data, whether for commercial or governmental purposes, is subject to compliance obligations. The specific compliance requirements will vary depending on the type of organization, the data they handle, where they operate, and which countries their customers are in.

CHAPTER 3:

Consequences of Non-Compliance

The consequences of non-compliance with cybersecurity regulations can be severe, and companies and individuals, especially senior management, can be liable. Repercussions include:

FINANCIAL PENALTIES: Regulators can impose substantial fines, significantly impacting an organization's bottom line.

For example, violating the US Health Insurance Portability and Accountability Act (HIPAA) can result in fines of up to $1.5 million. Organizations violating the EU's General Data Protection Regulation (GDPR) can face fines of up to €20 million or 4% of their global annual turnover.

$1.5 M
HIPPA Fine (max)

€20 M
or 4%
GDPR Fine (max)

LEGAL ACTIONS: Non-compliance may result in criminal or civil legal actions, including lawsuits from affected individuals or organizations and charges such as fraud or negligence.

REPUTATION DAMAGE: A data breach or other cybersecurity incident can damage an organization's reputation, leading to lost customers, decreased sales, and other financial losses.

OPERATIONAL DISRUPTION: A cyberattack can cause downtime and system outages, rendering critical business processes and services inaccessible, and investigations, system repairs, and customer notifications can divert resources, impacting productivity and profitability.

CHAPTER 4:

Data Protection Regulations

Data protection regulations apply to different data types, with requirements varying depending on jurisdictions and the kind of data being collected and processed. However, rules tend to govern three specific types of data.

PERSONAL DATA OR PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Data (EU) or Personal Identifiable Information (USA) includes any data that can be used to identify an individual, such as names, addresses, social security numbers, and email addresses. Regulations like GDPR in the EU and CCPA in California focus on protecting Personal Data.

PROTECTION REQUIREMENTS: Regulations mandate robust protection measures for Personal Data, including encryption, access controls, secure storage, and stringent data breach notification requirements. Organizations must obtain explicit consent for collecting and processing Personal Data and give individuals the right to access and delete their data.

PROTECTED HEALTH INFORMATION (PHI)

PHI includes health-related data, such as medical records and test results. Most developed countries have laws that regulate data privacy in healthcare, including HIPAA in the USA, the Patient Data Protection Act in Germany, and the Health Information Privacy Code in New Zealand.

PROTECTION REQUIREMENTS: Regulations mandate uncompromising security and privacy controls for PHI, including encryption, access logs, and auditing. To comply with HIPAA, for example, organizations must designate a person to oversee compliance. Breach notification requirements are strict, requiring prompt reporting to affected individuals and regulatory authorities.

PAYMENT AND FINANCIAL INFORMATION

Financial data, such as credit card numbers and bank account details, is subject to regulations like the Payment Card Industry Data Security Standard (PCI DSS), which ensures the secure handling of financial information, or the USA's Gramm-Leach-Bliley Act that requires financial institutions to explain their information-sharing practices to their customers in addition to safeguarding data.

PROTECTION REQUIREMENTS: Compliance with PCI DSS includes securing payment card data during storage, transmission, and processing. This involves encryption, secure network configurations, access controls, regular security assessments, and compliance reporting. Organizations must not store sensitive payment data unless necessary, reducing the risk of data breaches.

CHAPTER 5:

The Challenges of Compliance

Security frameworks are complex due to their multifaceted nature, making compliance a significant task for organizations of all sizes. It's a resource-intensive process that demands time and a substantial budget to cover the cost of hiring experts, vetting and due diligence procedures, and purchasing technology tools and solutions.

Effectively addressing compliance all starts with being aware of the common challenges businesses face.

COMPLYING WITH MULTIPLE AND CHANGING REGULATIONS

Multinational businesses, those with a single location but global clients, and even organizations that work across state lines need to navigate through a sea of intricate rules and standards, as they must comply with every applicable regulation.

Cybersecurity regulations are not static; they evolve to address emerging threats and technologies. Not staying up-to-date with these changes increases the risk of unintentional non-compliance, as organizations may be unaware of new requirements or fail to adapt quickly enough.

ADDRESSING AND HANDLING OVERLAPPING STANDARDS

Most organizations need to comply with multiple standards that have some overlapping requirements. For instance, GDPR and the Children's Online Privacy Protection Act (COPPA) address data privacy but have different scopes and target audiences.

An organization that targets European and USA markets and audiences of various ages must decipher how those two regulations intersect and implement measures that satisfy both, which can be intricate.

DEALING WITH THIRD-PARTY VENDORS

Almost every organization relies on third-party vendors, suppliers, or partners. Since businesses are ultimately responsible for safeguarding the data they collect and manage, whether stored in-house or by a third party, they must ensure external entities comply with relevant security and privacy standards.

Given that 51% of businesses have suffered a data breach caused by a third party, effectively managing this risk is crucial. Organizations must conduct due diligence, contractually bind vendors to compliance, and continuously monitor their compliance status.

THE AUDIT

Audits entail comprehensive assessments of security controls, data protection measures, and adherence to compliance frameworks. Organizations must also demonstrate their ongoing commitment to maintaining cybersecurity as regulations evolve.

Audits require meticulous preparation, documentation, and evidence collection, creating a demand for internal resources that can disrupt regular operations.

SENSITIVE INFORMATION

In addition to regulated data types, organizations must protect sensitive business or classified data, which may not fall directly under specific regulations but is just as critical for overall security.

With insider threats increasing by almost 50% over the last two years and 42% of insider threats related to the theft of IP, source code, and trade secrets, the need to actively combat corporate espionage and safeguard valuable information is no less important than adhering to government regulations.

CHAPTER 6:

Common and Major Cybersecurity Compliance Standards

Between jurisdiction-based laws, industry-specific regulations, and data protection laws, the number of compliance standards worldwide continues to grow every year. Here's a look at some of the most common cybersecurity compliance standards organizations across industries and regions must navigate. These standards are essential benchmarks for securing sensitive data, protecting privacy, and safeguarding against cyber threats.

You will also learn how a security operations center can aid in specific compliance regulations, closing critical regulatory requirements. For most businesses, from SMBs to enterprises, leveraging the expertise of a Security Operations Center (SOC) not only hardens their overall security posture but also offers continuous monitoring, threat detection, and incident response, as well as providing the necessary visibility and documentation to meet various compliance requirements. Organizations subject to specific regulations will even find that having a SOC is a requirement.

GDPR - GENERAL DATA PROTECTION REGULATION

Enforced in 2018

GDPR applies to any organization that collects or processes the personal data of individuals located in the European Economic Area (EEA), regardless of the organization's location. It governs how organizations must protect personal data, including obtaining consent before collecting or processing data, data breach notification, and data subject rights.

A security operations center (SOC) can help with GDPR compliance through security monitoring, incident response, and compliance reporting. A SOC can also help by providing training and awareness to employees on GDPR requirements and best practices, reducing the risk of human error and insider threats, two of the most common causes of GDPR data breaches.

Official Website

NIS 2 DIRECTIVE- NETWORK AND INFORMATION SYSTEMS DIRECTIVE

Enforced in 2022

The NIS 2 Directive applies to all operators of essential services (OESs) and digital service providers (DSPs) and expands on its predecessor to apply to all companies of all sizes. It aims to enhance the cybersecurity resilience of critical infrastructure and essential services.

Official Website

FISMA - FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Enacted in 2002

FISMA requires federal agencies and contractors to implement a comprehensive information security program to protect national information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction and sets guidelines for risk management and reporting requirements.

Official Website

FedRAMP - FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM

USA

Initiated in 2011

FedRAMP sets security standards for cloud service providers (CSPs) hosting US government data and provides a standardized approach to assessing, authorizing, and monitoring cloud services, ensuring they meet specified security requirements. FedRAMP requires cloud service providers to have a SOC.

Official Website

HIPAA - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

USA

Enacted in 1996

HIPAA applies to healthcare organizations, providers, covered entities, and their business associates. It's designed to protect the privacy and security of individually identifiable health information (PHI).

A SOC is recommended for all organizations that need to comply with HIPAA. It will provide security monitoring to detect suspicious activity that could indicate a data breach, incident response to investigate and contain a breach, and compliance reporting capabilities that demonstrate compliance.

Official Website

GLBA - GRAMM-LEACH-BLILEY ACT

USA

Enacted in 1999

GLBA, also known as the Financial Modernization Act of 1999, requires financial institutions to explain information-sharing practices to customers and protect the confidentiality, security, and integrity of sensitive customer information.

Official Website

CCPA - CALIFORNIA CONSUMER PRIVACY ACT

Enforced in 2020

CCPA applies to for-profit businesses that collect and process personal information of California residents, granting California residents the right to know what personal information businesses are collecting, to request that companies delete their data, and to opt out of the sale of their data.

Official Website

SEC CYBER DISCLOSURE - SECURITIES AND EXCHANGE COMMISSION

Enacted in 2011

SEC regulations require public companies and foreign private issuers to disclose material cybersecurity incidents within four business days and disclose their processes for assessing, identifying, and managing material cybersecurity risks.

Official Website

SOX - SARBANES-OXLEY ACT

Enacted in 2002

SOX applies to all publicly traded companies in the US, foreign companies that list their securities on a US stock exchange, and certain non-public companies, such as investment companies and broker-dealers. It mandates certain practices for financial reporting and corporate governance. It also ensures whistleblowers can safely disclose information and fraud that may harm investors.

SOX applies to all publicly traded companies in the US, foreign companies that list their securities on a US stock exchange, and certain non-public companies, such as investment companies and broker-dealers. It mandates certain practices for financial reporting and corporate governance. It also ensures whistleblowers can safely disclose information and fraud that may harm investors.

Official Website

DATA PROTECTION ACT 2018

Enforced in 2018

It supplements GDPR in the UK and applies to any organization that collects or processes the personal data of individuals in the UK. It sets out how organizations must protect personal data, obtain consent, and give individuals access to and control over their data.

Official Website

NIS REGULATIONS- NETWORK AND INFORMATION SYSTEMS REGULATIONS

Enforced in 2018

These regulations implement the NIS Directive and apply to operators of essential services (OESs) and digital service providers (DSPs) in the United Kingdom.

Official Website

CYBERSECURITY LAW OF 2017

Enforced in 2017

The law sets the requirements for how all organizations operating in China or collecting the personal information of individuals in China protect personal data. It requires network operators to store select data in China and allows Chinese authorities to spot-check a company's network operations.

Official Website (Translation)

PRIVACY ACT 1988

Enacted in 1988

The Privacy Act applies to government agencies and private sector organizations with an annual turnover of $3 million. It governs the processing of personal information, including data collection, use, disclosure, quality, and security.

Official Website

PDPA - PERSONAL DATA PROTECTION ACT

Enacted in 2012

The PDPA regulates the collection, use, and disclosure of personal data by any organization that collects or processes the personal data of individuals located in Singapore.

Official Website

PIPEDA - PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Enacted in 2000

PIPEDA requires Canadian and non-Canadian organizations that obtain personal data from residents to inform users of data handling practices and obtain consent to collect, use, and disclose personal information.

Official Website

KRITIS ACT - CRITICAL INFRASTRUCTURE LEGISLATION

Enacted in 2021

KRITIS requires operators of critical infrastructure in Germany to implement security measures to protect systems from cyber threats and report incidents to authorities.

Official Website

LGPD - GENERAL DATA PROTECTION LAW

Enacted in 2018

LGPD is Brazil's GDPR-inspired law. It applies to any person, legal entity, and government organization that processes the personal data of individuals located in Brazil and ensures data subject rights and data protection.

Official Website (Translation)

LFPDPPP – FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

Enacted in 2010

The PDPA regulates the collection, use, and disclosure of personal data by any organization that collects or processes the personal data of individuals located in Singapore.

Official Website

DATA PROTECTION LAW IN ARGENTINA

Enacted in 2000

PDPA applies to all people, legal entities, and foreign data controllers and processors that process the personal data of people in Argentina. It requires express consent to collect data and requires data controllers and processors to use measures to detect unauthorized access or amendment to personal data.

Official Website (Translation)

PERSONAL DATA PROTECTION LAW

Enacted in 1999

Chile's data protection law regulates the processing of personal data by public and private organizations. It stipulates that personal data can only be processed if permitted by law, such as labor or health care laws, or by an individual's informed consent.

Official Website (Translation)

LAW ON PERSONAL DATA PROTECTION

Enacted in 2011

Peru's data protection law governs the processing of personal data by public and private sector entities. It requires organizations to obtain informed consent and adopt measures to guarantee the security of personal data.

Official Website (Translation)

PERSONAL DATA PROTECTION LAW

Enacted in 2012

The law guarantees individuals' rights to know, update, and rectify information collected about them. It applies to all public or private individuals and corporations who process personal data, whether collected in Colombia or abroad, but not to data regulated under Law 1266. Organizations must preserve proof of consent and allocate a department or person responsible for personal data matters.

Official Website (Translation)

PCI DSS – PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

(Applies wherever credit card payments are processed)

Introduced in 2004

PCI DSS sets security standards for all entities that accept, transmit, or store payment card data. It sets the requirements for how organizations must protect payment card data, including implementing strong security controls to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of data.

A SOC can play a valuable role in helping organizations comply with the PCI DSS. By providing security monitoring, incident response, and compliance reporting capabilities, a SOC can help organizations identify and mitigate risks, respond to incidents quickly and effectively, and build trust with customers and stakeholders by demonstrating compliance.

Official Website

ISO 27000 SERIES

First Standard Released in 2005

The ISO 27000 series provides a framework for organizations to implement and manage information security management systems (ISMS), which helps protect their information assets from unauthorized access, use, disclosure, disruption, modification, or destruction.

Official Website

CHAPTER 7:

Building a Cybersecurity Compliance Program

A cybersecurity compliance program is a set of policies, procedures, and controls an organization implements to ensure compliance with applicable regulations. A well-designed compliance program can help an organization reduce the risk of a cyberattack, protect its data, and avoid fines and penalties.

By following eight essential steps, businesses can build robust compliance programs.

1 MAP FRAMEWORKS

Identify all applicable cybersecurity frameworks and regulations, considering factors such as location, industry, and the nature of the data handled. Then, map requirements to existing security measures to identify gaps in security controls. Consider available resources and the processes needed to achieve compliance.

2 CONDUCT A RISK ASSESSMENT

Perform a comprehensive risk assessment to identify potential cybersecurity risks and vulnerabilities. Prioritize these risks based on their potential impact on the organization and create a plan to address them by implementing new security controls, updating existing controls, or changing security policies and procedures.

3 ESTABLISH GOVERNANCE

Define roles and responsibilities within your organization for managing and maintaining compliance and establish reporting lines for cybersecurity matters. Governance also encompasses creating policies, procedures, and guidelines that outline how compliance requirements will be met, monitored, and enforced.

4 VET THE DIGITAL SUPPLY CHAIN

Evaluate the cybersecurity posture of your third-party vendors and suppliers, including their data protection measures, security controls, and compliance with relevant regulations. Due diligence also extends to contractual agreements that should include specific security requirements, audit rights, and breach notification obligations.

5

KEEP RANSOMWARE POLICIES UP TO DATE

An up-to-date ransomware policy ensures the organization has clear, effective procedures for preventing, detecting, and responding to ransomware incidents. As compliance standards adapt to address emerging cybersecurity risks, adhering to the latest ransomware policies ensures that the organization remains compliant with evolving regulatory requirements.

6

ESTABLISHING CONTINUOUS MONITORING

Continuous monitoring is the best way to gain real-time visibility into an organization's security posture, enabling the timely detection and response to security threats and compliance violations. CYREBRO's SOC Platform can play a pivotal role by actively and continuously monitoring network traffic, systems, and data for anomalies, vulnerabilities, and potential breaches. CYREBRO's advanced technologies, threat intelligence, and skilled analysts can identify security incidents quickly and mitigate risks before they lead to a cyberattack.

7

ESTABLISH AN ENHANCED RESPONSE AND INCIDENT RECOVERY PLAN

An enhanced response and incident recovery plan should outline the actions to take in the event of a security incident, which is essential to minimize the impact, comply with mandatory breach notification requirements, and swiftly restore normal operations.

A well-integrated SOC with real-time threat detection and incident response capabilities can help an organization identify security incidents, assess their severity, execute predefined incident response procedures, and preserve evidence for potential legal and regulatory actions - all of which are vital for maintaining data security and regulatory compliance.

8

CREATE A CULTURE OF SECURITY

Ninety-five percent of security issues stem from human error, which means if organizations establish a security culture, most incidents could be avoided. When cybersecurity becomes ingrained in the company culture, employees are more likely to adhere to compliance policies, report security concerns, and actively maintain a secure environment, strengthening compliance efforts and reducing risks.

CHAPTER 8:

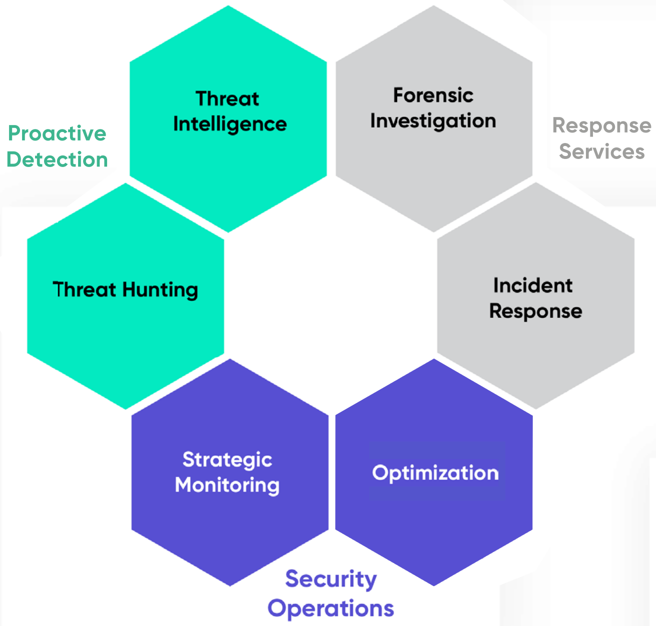
A Path to Compliance and Beyond

Achieving and maintaining compliance is an ongoing journey. Cybersecurity compliance is not just a legal obligation; it's a fundamental component of a robust cybersecurity strategy. Those responsible must stay informed about changes in regulations and emerging threats, as a lack of awareness is not an acceptable excuse for non-compliance; neither is a lack of resources.

Regulatory compliance has grown to reach and affect far beyond a selected few. A vastly digital and connected globe has enabled an attack surface that must be regulated and kept safe, no matter the industry, region, or business size.

Organizations must dedicate internal resources to regularly assess and address compliance as regulatory changes take effect. Those that cannot, which is the vast majority of SMBs and a fair number of enterprises, should leverage the power of a trusted SOC.

With a powerful SOC Platform like CYREBRO at the helm, organizations can simplify and prove compliance, harden their overall cybersecurity posture, and protect their organization from an inevitable cyber threat.



To learn more about CYREBRO's capabilities

Learn more